# Truly noiseless probabilistic amplification

# Truly noiseless probabilistic amplification

Vedran Dunjko[1,2] and Erika Andersson[1]
[1]*SUPA, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, United Kingdom*
[2]*Division of Molecular Biology, Ruđer Bošković Institute, Bijenička cesta 54, P.P. 180, 10002 Zagreb, Croatia*
(Received 26 June 2012; published 18 October 2012)

Most of the schemes for "noiseless" amplification of coherent states, which have recently been attracting theoretical and experimental interest, share a common trait: The amplification is not truly noiseless, or perfect, for nonzero success probability. While this must hold true for all phase-independent amplification schemes, in this work we point out that truly noiseless amplification is indeed possible, provided that the states which we wish to amplify come from a finite set. Perfect amplification with unlimited average gain is then possible with finite success probability, for example, using techniques for unambiguously distinguishing between quantum states. Such realizations require only linear optics, no single-photon sources, and no photon counting. We also investigate the optimal success probability of perfect amplification of a *symmetric* set of coherent states. There are two regimes: low-amplitude amplification, where the target amplitude is below one, and general amplification. For the low-amplitude regime, analytic results for the optimal amplification success probabilities can be obtained. In this case a natural bound imposed by the ratio of success probabilities of optimal unambiguous discrimination of the source and amplified states can always be reached. We also show that for general amplification this bound cannot always be satisfied.

DOI: 10.1103/PhysRevA.86.042322 PACS number(s): 03.67.−a, 42.50.Dv, 42.50.Ex

## I. INTRODUCTION

There has recently been widespread theoretical and experimental interest in schemes for "noiseless" amplification of coherent states [1–6]. These schemes aim to implement the operation $|\alpha\rangle \rightarrow |g\alpha\rangle$, for $g > 1$ and any $\alpha$. This is not possible to achieve perfectly with unit probability, but can be done probabilistically with arbitrarily high fidelity. Noiseless amplification could, for example, be used in quantum repeaters or for entanglement purification through "breeding" larger Schrödinger cat states from "kittens" by probabilistically transforming $N_{\pm}(|\alpha\rangle \pm |-\alpha\rangle)$ into $N'_{\pm}(|g\alpha\rangle \pm |-g\alpha\rangle)$ with high fidelity.

Common to all existing schemes is that the amplification is not truly noiseless, or perfect, for nonzero success probability. That is, the fidelity approaches unity only in the limit of vanishing success probability. This must, in fact, hold for any phase-independent amplification scheme [5]. The suggested schemes achieve higher fidelity for smaller $\alpha$ or smaller gain, but it is only if either $|\alpha\rangle = |0\rangle$ or $g = 1$ that the fidelity can be 100% for nonzero success probability, in which case, of course, no amplification actually takes place. For experimental realizations, the overall success probability is usually not even quoted, and only the fidelity in case of successful operation is reported as a figure of merit. A complete and fair comparison of the different schemes is therefore difficult. The success probability, especially for schemes that involve single-photon states as resources, is nevertheless usually very low.

In this paper we want to point out that, in contrast to existing theoretical and experimental schemes, there *is*, in fact, a way to achieve truly noiseless amplification, that is, 100% fidelity, also for finite nonzero success probability and finite nonzero coherent state amplitudes. This is possible if one relaxes the demand that the amplification should work for any $|\alpha\rangle$ and instead selects any finite number of coherent states that one wants to amplify perfectly. The restriction to a finite set of states need not be serious, since many quantum information and communication protocols use a selected set of states, including quantum cryptography [7–9], blind quantum computing [10], and quantum digital signatures using coherent states [11,12]. For example, the set of symmetric coherent states $|\alpha e^{im2\pi/N}\rangle$, where $\alpha$ is fixed and $m = 1,2,\ldots,N$, may be amplified truly perfectly with nonzero success probability.

In fact, any set of linearly independent quantum states, coherent or other, may be amplified or cloned perfectly with a finite nonzero probability of success. This follows from the fact that linearly independent states may be unambiguously distinguished from each other with finite success probability [13]. Perfectly identifying a quantum state clearly allows us to fabricate an unlimited number of copies or, equivalently, to prepare a state with the same phase and arbitrarily high amplitude. Hence, it is not only possible to perfectly amplify any linearly independent set of states, but the average gain of truly noiseless probabilistic amplification can be *arbitrarily high*, since the success probability times the gain is unlimited. Moreover, unambiguous state discrimination of coherent states may be realized using only linear optics and non-photon-number-resolving photodetectors, without using auxiliary nonclassical states [14,15]. The same resources allow also realization of perfect amplification based on unambiguous state discrimination (USD).

When discussing amplification, the so-called classical linear amplifier is often used as a benchmark [4]. This is a measure-and-prepare approach to amplification or cloning, where the state is first estimated and, based on this, the amplified state prepared. Depending on which states we wish to amplify or clone, however, the optimal measure-and-prepare classical amplifier protocol will be different. Existing amplification protocols for coherent states are phase independent [1–6] or consider some other continuous distribution of coherent states [16–20]. For a continuous input distribution, the realized amplification fidelity can never be perfect. In contrast to this, we consider a restricted setting where the

 

inbound set of states is finite and linearly independent. This will be related to a *different* measure-and-prepare protocol than phase-independent amplification, in other words, to a different classical amplifier.

If we do not require arbitrarily high gain, then the success probability can be higher than for schemes based on USD. For amplification of symmetric sets of coherent states, results on transforms between sets of symmetric states [21] are key to working out what processes are possible. Such transforms might be termed "umbrella transforms," if we visualize the symmetric states as the ribs of an umbrella in a space of suitable dimensionality. A probabilistic transform that decreases pairwise overlaps—one example being noiseless amplification—may then be thought of as "opening the umbrella." We are concerned with the theoretical limits of limited-gain perfect amplification of a restricted set of possible input states, in particular, the optimal success probabilities of such transforms.

The paper is organized as follows. In Sec. II, we briefly review unambiguous discrimination of coherent states using linear optics and discuss how to use this for truly noiseless amplification. Definitions related to transformations between sets of quantum states are given in Sec. III. In Sec. IV, we investigate truly noiseless amplification of coherent states, for finite gain, by viewing it as a transform between symmetric sets of states. As already mentioned, the success probability can then be higher than for procedures that use state discrimination. It turns out that there are two regimes: small-amplitude amplification, where the amplitudes of both initial and amplified states are below one, and a general regime where the amplitude of the final states, or of both initial and final states, are above one. As shown in Ref. [21], transforms between sets of states may be "leaky" or "leakless," depending on whether there is an extra "leak" state correlated with the desired output in the case of success. It turns out that in the small-amplitude regime, the optimal umbrella transforms for noiseless amplification are leakless, whereas in the general regime they may be leaky. We finish with a discussion.

## II. AMPLIFICATION OF COHERENT STATES USING LINEAR OPTICS

Ivanovic [22], Dieks [23], and Peres [24] realized that two nonorthogonal quantum states can be unambiguously distinguished from each other with a certain probability. That is, if the measurement succeeds, the result is always correct, but there is a chance that the measurement fails, giving an inconclusive result. The failure probability for the optimal procedure is equal to the overlap between the two quantum states. In the completely general case, optimal unambiguous measurements are not easy to find analytically [25,26], but such a measurement is at least possible as soon as at least one of the quantum states is linearly independent of the others [13].

For two coherent states $|\alpha\rangle$ and $|-\alpha\rangle$, the optimal measurement may be realized using only linear optics [14]. The state to be identified, $|\pm\alpha\rangle$, is directed onto a balanced beam splitter, with a fixed state $|\alpha\rangle$ incident on the other input port. If the phase relationships between output and input ports are arranged so that the beam splitter transforms $|\alpha\rangle_1 \otimes |\beta\rangle_2$ to $|(\alpha+\beta)/\sqrt{2}\rangle_1 \otimes |(\alpha-\beta)/\sqrt{2}\rangle_2$, we see that if the state to be identified was $|\alpha\rangle$, then output port 1 will contain $|\sqrt{2}\alpha\rangle$ and port 2 will be empty, and if it was $|-\alpha\rangle$, then output port 1 will be empty and output mode 2 will contain $|-\sqrt{2}\alpha\rangle$. By detecting photons in the output ports, we can therefore unambiguously tell whether the state in input port 1 was $|\alpha\rangle$ or $|-\alpha\rangle$. Since any coherent state contains a vacuum component, we may not see any photons at all, which corresponds to the inconclusive outcome. The probability for this is $\langle 0|\sqrt{2}\alpha\rangle = \langle -\alpha|\alpha\rangle = \exp(-|\alpha|^2)$, which is the optimal (minimal) failure probability. Clearly, no photon counting is required, only being able to tell the difference between the vacuum and any nonzero number of photons.

For a balanced beam splitter with other phase relationships, we can adjust the phase of the fixed state in input port 2 so that the procedure still works. Also, if the two states to be distinguished are not $|\pm\alpha\rangle$ but $|\alpha\rangle$ and $|\beta\rangle$, then we can precede the described measurement with displacement of the unknown input mode, containing either state $|\alpha\rangle$ or state $|\beta\rangle$, by $-(\alpha+\beta)/2$ using a beam splitter, and then distinguish $|\pm(\alpha-\beta)/2\rangle$ using the technique above.

This unambiguous measurement may be used for perfect amplification as shown in Fig. 1, where the first box shows a suggested way to prepare the states to be distinguished, and the second box shows the unambiguous measurement itself. The fact that we need to specify the phases of $|\pm\alpha\rangle$ implies that there exists a phase reference beam, which we, without loss of generality, assume to be $|\beta\rangle$, where $\alpha$ and $\beta$ have the same phase, but different amplitude; a strong reference beam would have $|\beta| \gg |\alpha|$. The fixed state $|\alpha\rangle$ in input mode 2 is likely also split off this reference beam, as shown in Fig. 1. Conditional on whether the state is identified as $|\alpha\rangle$ or $|-\alpha\rangle$, we implement the corresponding phase shift on the reference beam, giving the amplified state. The gain is then only limited by how strong the reference beam is. Alternatively, we could amplify relative to some other reference beam, not necessarily with the same phase as $|\alpha\rangle$ (but we still need the fixed state $|\alpha\rangle$ with the correct phase in input mode 2 for the unambiguous measurement).

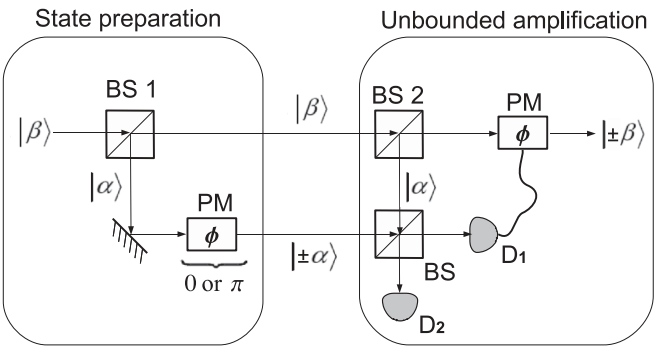


FIG. 1. Truly perfect amplification of the states $|\pm\alpha\rangle$ based on unambiguous discrimination, where we assume that $|\beta| \gg |\alpha|$. The beam splitters denoted BS 1 and BS 2 split off a minor fraction of the strong beam $|\beta\rangle$ of amplitude of norm $|\alpha|$. The beam splitter BS is balanced, and boxes labeled PM denote phase modulators. The amplification procedure fails only if both detectors $D_1$ and $D_2$ fail to detect a photon.

A similar procedure is possible for distinguishing between more than two coherent states using linear optics, but will then not attain the optimal success probability [15]. In short, if there are $N$ possible different states, then we can split the unknown state in $N$ beams using a multiport and test each component against one of the possible states (with amplitude suitably scaled down) using a beam splitter similar to that described above for two coherent states. If we manage to rule out all but one of the possible states, then we have unambiguously identified the input state as the remaining one. (Actually, we would only need to split the state to be identified in $N-1$ components, since if we manage to rule out all but one of the possible states, then the state must have been the remaining one.) The success probability of this procedure is nonzero, but not optimal. It can be somewhat improved by splitting the original state in $M$ copies, with $M \to \infty$, still using only linear optics [15].

Any such procedure to unambiguously distinguish a finite number of coherent states may be used to noiselessly amplify them with a finite success probability and gain limited only by the strength of a reference beam, similar to amplification of two coherent states illustrated in Fig. 1. If we manage to identify the state, we implement the corresponding phase shift on the reference beam. Although this requires only linear optics and detectors that do not resolve photon numbers, the disadvantage is that such a procedure cannot be used to amplify a superposition of the possible incident states. This obviously limits the usefulness when the superposition is important, such as when "breeding" larger cat states in order to enhance entanglement.

It is nevertheless, in principle, possible to realize truly noiseless amplification in such a way that superpositions are preserved. This is because one can, in principle, realize USD in two steps. First, one probabilistically transforms the selected set of nonorthogonal states into orthogonal ones without destroying possible superpositions of the states in the set, and this is followed by a measurement to distinguish the different orthogonal states. Truly noiseless amplification that preserves superpositions can then be achieved by omitting the final measurement, and only registering whether the first step succeeded or failed [how this works is also clarified by Eq. (1) in the following section].

If the states to be amplified are symmetric to start with, then it follows from results in Ref. [21] that the success probability can be made independent of the initial state, and therefore the weights of the states in the superposition will be preserved. If the set of states is not symmetric, then the success probabilities for different states in the "source" set may not be equal. Amplification that preserves the superposition but reweights the individual states is then still possible. Also, if we base the procedure on USD, then the amplified states in the superposition will be orthogonal, corresponding to infinite coherent state amplitude (the unambiguous measurement, if completed, would give us perfect knowledge about which state was prepared, if only one of the initial states was prepared). Alternatively, if the amplitude of the amplified states is below one, then amplification that preserves superpositions is also possible, since then a leakless transform is possible, as we show in Sec. IV A (the concept of leak is introduced in the next section). We leave it open whether superposition-preserving truly noiseless amplification of coherent states could be realized using only linear optics.

Alternatively, we could remove the detectors and the strong reference beam $|\beta\rangle$ in the second box in Fig. 1 and view the state exiting from the beam splitter labeled "BS", after combining the incident state $|\pm\alpha\rangle$ with the fixed state $|\alpha\rangle$, as an "amplification," with gain $\sqrt{2}$, of the incident state. This amplification occurs with unit probability, that is, it is deterministic, and transforms a superposition $N_\pm(|\alpha\rangle_1 \pm |-\alpha\rangle_1)$ into $N'_\pm(|\sqrt{2}\alpha\rangle_1 \otimes |0\rangle_2 \pm |0\rangle_1 \otimes |-\sqrt{2}\alpha\rangle_2)$. The deterministically amplified state will then be a superposition of different output modes. However, the overlap between the incident states $|\pm\alpha\rangle_1 \otimes |\alpha\rangle$ is necessarily the same as the overlap between the states $|\sqrt{2}\alpha\rangle_1 \otimes |0\rangle_2$ and $|0\rangle_1 \otimes |-\sqrt{2}\alpha\rangle_2$. Thus, it is questionable if this process really could be called amplification, without subsequently combining the amplified states into the same spatial mode. That can only be done probabilistically, since otherwise we would be able to deterministically decrease the overlap of two quantum states, which is impossible.

Amplification with, in principle, unlimited gain will necessarily have the same optimal success probability as USD. We now proceed to investigate the optimal success probabilities and other properties of the amplification transforms for specified finite levels of gain. For this, we first need to state some definitions related to transforms between sets of quantum states.

## III. TRANSFORMS BETWEEN SETS OF STATES

In the previous section, we considered perfect amplification with unlimited gain, based on USD techniques. We noted that if USD is viewed as a heralded transformation from nonorthogonal to orthogonal states, followed by a measurement to distinguish between these states, there is nothing forbidding amplification which also preserves superpositions. In contrast to this, we now consider perfect amplification of a finite set of coherent states, with *limited* gain. Our approach is based on viewing amplification as a transformation between finite sets of states, and our goal to find the limits of success probability for such transforms, that is, for truly perfect amplification.

We consider two sets of $N$ pure states, called the *source* and *target* sets, denoted (respectively)

$$A = \{|a_i\rangle\},\ B = \{|b_i\rangle\},$$

and a heralded probabilistic transform $\mathcal{T}$, which for input state $|a_i\rangle$ produces the state $|b_i\rangle$ with probability $p_i$, and a $|\text{Fail}\rangle$ state with probability $1-p_i$. By Theorem 3 in Ref. [27] such a transform exists if and only if there exists a unitary transform $U$ performing

$$U|a_i\rangle = \sqrt{p_i}|b_i\rangle|\psi_i\rangle|0\rangle + \sqrt{1-p_i}|\text{Fail}\rangle|\phi_i\rangle|1\rangle, \quad \forall\, i \qquad (1)$$

for some sets of states $L = \{|\psi_i\rangle\}_N$ and $R = \{|\phi_i\rangle\}_N$. The states $|0\rangle$ and $|1\rangle$ are orthogonal. To complete the realization of $\mathcal{T}$, after the application of $U$ the third register is measured in this basis, and, optionally, the second register may be traced out.

When the transform succeeds, the state $|b_i\rangle$ is generated along with a state $|\psi_i\rangle$, possibly correlated with the input state.

This state leaks additional information about $i$; hence, the set $L$ is called the *leak*. When the transform fails, the constant state $|\text{Fail}\rangle$ is produced along with the state $|\phi_i\rangle$, which may be correlated with the source state, and may be used to attempt a reconstruction of the target state $|b_i\rangle$. This set of states $R$ we call the *redundancy*. The leak (redundancy) states are not correlated with the input state if and only if the states in the leak (redundancy) are identical for all source states, up to global phase. If the success probabilities do not depend on the input state, the transform is called *uniform*. For uniform transforms (of success probability $p$) the criterion (1) may be rewritten, in terms of the Gram matrices of the sets $A$, $B$, $L$, and $R$, respectively, as

$$G_A = p\, G_B \circ G_L + (1-p)\, G_R, \tag{2}$$

where $\circ$ denotes the Hadamard (pointwise) matrix product. The Gram matrix of a set of states $\{|c_i\rangle\}$ is defined as the square matrix with elements $\langle c_i|c_j\rangle$.

Finally, a finite set of states is *symmetric* if there exists a fixed unitary which, when applied on the $i$th state, produces the $(i+1 \bmod N)$th state. Symmetric states are interesting as they often appear in quantum protocols (e.g., many quantum key distribution schemes [7–9] and in blind quantum computing [10] and quantum digital signature schemes with coherent states [11,12]).

## IV. AMPLIFICATION AS STATE TRANSFORMS

If the source set of coherent states we wish to amplify perfectly is known, and the required gain $g > 1$ is preset, then the amplification procedure becomes a particular type of state transform which has been studied in Ref. [21]. Here, we assume that the source set of coherent states is a symmetric set of $N$ states. The source and target states are then

$$A = \{|a_i\rangle := |e^{i\theta_k}\alpha\rangle\}_{k=0}^{N-1}, \quad B = \{|b_i\rangle := |e^{i\theta_k}\beta\rangle\}_{k=0}^{N-1}, \tag{3}$$

where $\theta_k = 2k\pi i/N$ and $\beta = g\alpha$. An amplification transform takes states from set $A$ to corresponding (amplified) states in set $B$ and, without loss of generality, we define the amplitudes $\alpha$ and $\beta$ to be real positive numbers. The question is with what success probability such amplification is possible.

Since the set $A$ is a set of linearly independent states, using state discrimination one can always perform a measure-and-prepare procedure and, in fact, reach any desired, unlimited gain. Thus, the lower bound on the success of an amplification procedure is given by $d_A$, denoting the success probability of USD of the states in $A$. If we also take into the account the probability of unambiguous discrimination of states in $B$, an upper bound of the success probability of amplification can be derived. If $d_A$ and $d_B$ are the respective probabilities of optimal unambiguous discrimination of states in the sets $A$ and $B$, then the corresponding amplification transform cannot succeed with a probability higher than

$$p_{\text{up}} = \frac{d_A}{d_B} \tag{4}$$

as a higher success probability would violate the optimality of $d_A$. Similar methods have been used to bound the success probability of decreasing the overlap of two quantum states, which includes state-dependent cloning or two states [28]. Similarly, one could derive other bounds by observing the optimal probabilities of minimum error measurements [29] on the sets $A$ and $B$, or, in fact, any measurement optimizing any other figure of merit (e.g., maximal mutual information, maximum likelihood, etc.).

As we will show, the bound $p_{\text{up}}$ can, in fact, be reached for source and target amplitudes below one, whereas for target state amplitudes above one it cannot always be saturated. The techniques we use have been developed in Refs. [21,27,30]. By the results given in Refs. [27,30], an amplification transform succeeding with probability $p$ exists if the equality given in Eq. (2) is satisfied for some Gram matrices of states [31] $G_L$ and $G_R$ and where $G_A$ and $G_B$ are the Gram matrices of the source and amplified coherent states, respectively. Since $A$ and $B$ are symmetric sets of states, the matrices $G_A$ and $G_B$ are circulant [32], and hence diagonalize in the unitary discrete Fourier transform basis, which is given by the columns or rows of the unitary discrete Fourier matrix of appropriate size $N$,

$$u_{\text{DFT}} = 1/\sqrt{N}\left[\exp\ \frac{-2\,(p-1)\,(q-1)\,i\pi}{N}\right]_{p,q}. \tag{5}$$

Moreover, by Lemma 4 in Ref. [21], if there exists any amplification procedure for symmetric states succeeding with some success probability, then there exists an amplification procedure succeeding with the same success probability, where the leak and redundancy are symmetric sets of states.

Thus, in order to find the optimal success probability, we may assume that all the matrices appearing in the existence criterion (2) are circulant, and they all diagonalize in the unitary discrete Fourier transform basis. Criterion (2) may then be written in terms of vectors containing the eigenvalues of the Gram matrices as

$$\lambda_A = p\lambda_B * \lambda_L + (1-p)\lambda_R. \tag{6}$$

In this expression the vector $\lambda_X$ contains the diagonal elements of the matrix $u_{\text{DFT}}^{\dagger} G_X u_{\text{DFT}}$, which is diagonal when $X$ is a symmetric set of states, and $*$ denotes the circular convolution of vectors, defined componentwise as

$$(\lambda_B * \lambda_L)_i = \frac{1}{N}\sum_{j=0}^{N-1} (\lambda_B)_j (\lambda_L)_{[(N-j+i) \bmod N]}. \tag{7}$$

For more details on the construction above, see Ref. [21].

All the results we give rely on the properties of the spectrum of Gram matrices of coherent states which we give collectively in the Appendix for convenience. As this spectrum has roughly two regimes of behavior, depending on the amplitudes $\alpha$ and $\beta$ being below or above one, we separately address two distinct cases: small-amplitude amplification (where $0 < \alpha \leqslant \beta \leqslant 1$) and general amplification (all other amplitude combinations). We begin by considering the scenario where both input and output amplitudes are small, that is, less than one. From a practical standpoint, low-amplitude amplification is of high importance since weak coherent states are often used in quantum information protocols. For sufficiently high amplitudes (also depending on $N$, that is, how many states there are), the symmetric sets of coherent states are effectively *classical*, that is, mutually almost orthogonal, and can be

reliably distinguished. From a theoretical viewpoint, adhering to low amplitudes allows us to derive useful properties which do not hold for higher amplitudes.

### A. Small-amplitude amplification

If the amplitudes $\alpha$ and $\beta$ of sets of symmetric coherent states $A$ and $B$, respectively, satisfy $|\alpha| < |\beta| < 1$, the following two properties hold for the spectra of their corresponding Gram matrices $G_A$ and $G_B$.

*Property 1*. The eigenvalues of $G_A$ appear in strictly decreasing order, where the order is induced by the order of the diagonal elements of the diagonalized matrix obtained by the conjugation of $G_A$ with the $u_{\mathrm{DFT}}$ matrix (cf. Lemma 2 below). This does not hold for higher amplitudes.

*Property 2*. The quotient of the last eigenvalues of $G_A$ and $G_B$ is smaller than the quotient of any other two corresponding eigenvalues (cf. Lemma 3 below and the derivation preceding it). Again, this holds only in the small-amplitude regime.

For proofs, please see the Appendix.

Property 2 above implies that the upper bound on the optimal success probability $p_{\mathrm{up}}$ in the low-amplitude regime, addressed in the beginning of this section, is reached in the leakless scenario, as we now show. First, we note the link between the optimal success probability $d_S$ of uniformly and unambiguously discriminating a set of pure states $S$ and the spectrum of the Gram matrix $G_S$ of $S$: The optimal success probability $d_S$ is equal to the smallest eigenvalue of $G_S$ (this is easily derived from the results in Refs. [27,30,39], as was done in Ref. [21]). Also, the sufficient criterion (6) for the existence of a probabilistic leakless transform taking the states from $A$ to $B$ where both sets of states are symmetric, succeeding with the probability $p$, can be written as

$$\lambda_A - p\lambda_B \geqslant 0, \tag{8}$$

where $\lambda_A$ and $\lambda_B$ are the vectors of eigenvalues of matrices $G_A$ and $G_B$, as discussed in the previous section. To see this, note that if the transform is leakless, then $\lambda_B * \lambda_L = \lambda_B$. The maximal possible $p$ is then equal to $\min_j(\lambda_A^j/\lambda_B^j)$, where $\lambda_A^j$ and $\lambda_B^j$ are the $j$th components of the vectors $\lambda_A$ and $\lambda_B$, respectively. Now, by the second property, this minimum is attained for the last eigenvalues (i.e., $j = N-1$), which is exactly the upper bound $p_{\mathrm{up}}$. Thus, there exists a leakless transform saturating the upper bound of the success probability of amplification $p_{\mathrm{up}}$.

Moreover, it can be shown by using Property 1 that this bound is saturated *only* by a leakless transform in the small-amplitude regime. From criterion (6), if there exists an amplification transform with a nontrivial leak, succeeding with some probability $p$, then the relation

$$\lambda_A - p\lambda_B * \lambda_L \geqslant 0 \tag{9}$$

holds, where $\lambda_L$ is the vector of eigenvalues of the Gram matrix of the leak. Note that here we are assuming that the Gram matrix of the leak diagonalizes in the unitary discrete Fourier transform basis, which is justified without the loss of generality due to Lemma 4 in Ref. [21]. If the leak is not trivial (not a fixed state) then $\lambda_L$ is a vector of non-negative numbers adding up to $N$, at least two of which are not zero. Then note that the vector $\lambda_C = \lambda_B * \lambda_L$ contains the (normalized) weighted sums of the components of $\lambda_B$, the weights being the elements of $\lambda_L$ [see the definition of the discrete convolution of vectors in expression (7)]. Since the smallest component $\lambda_B^{\min}$ is the unique last component of $\lambda_B$ (for $|\beta| < 1$ by Property 1), and at least two of the elements of $\lambda_L$ are nonzero, the last component of $\lambda_C$ is strictly greater than $\lambda_B^{\min}$. However, then it holds that

$$p \leqslant \frac{\lambda_A^{N-1}}{\lambda_C^{N-1}} < \frac{\lambda_A^{N-1}}{\lambda_B^{\min}} = \frac{\lambda_A^{\min}}{\lambda_B^{\min}}. \tag{10}$$

Hence, the success probability of any leaky (nonleakless) amplification transform for low amplitudes is strictly less than optimal.

Thus, we have shown that small-amplitude amplification can be done optimally, that is, saturating the obvious upper bound of the success probability $p_{\mathrm{up}}$, and that this optimal transform is always leakless. The amplification procedure properties change significantly when one is interested in amplification involving states with amplitudes above unity, as we see next.

### B. General amplification

For "any amplitude" amplification, that is, when $\beta > 1$, we no longer have the convenient properties given in the previous section. In particular, optimal transforms can be leaky, in which case the upper bound $p_{\mathrm{up}}$ derived through the probabilities of unambiguous discrimination [see expression (4)] sometimes no longer can be reached. More formally, we have the following lemma.

*Lemma 1*. Let $\lambda_B^{\min}$ be the smallest eigenvalue of the Gram matrix of the target, amplitude-amplified, symmetric set of coherent states. Then if $\lambda_B^{\min}$ is a unique smallest eigenvalue then an optimal amplification transform with a nontrivial leak does not saturate the upper bound $p_{\mathrm{up}}$.

*Proof*. Let $c_j$ denote the $j$th component of the vector $\lambda_C = \lambda_B * \lambda_L$, where $\lambda_B$ and $\lambda_L$ are vectors of eigenvalues of the Gram matrices of the target states and the leak states. Let $c^{\min} = \min_j c_j$. Then, if $\lambda_B^{\min}$ is unique, and since $\lambda_B * \lambda_L$ contains the (normalized) weighted sums of the components of $\lambda_B$, the weights being the elements of $\lambda_L$, and at least two weights are not zero, it holds that $\lambda_B^{\min} < c^{\min}$.

Let $p$ be the success probability of an optimal amplitude amplification transform with the leak characterized by $\lambda_L$. Then it holds that

$$\lambda_A - p\lambda_C \geqslant 0. \tag{11}$$

Also, due to optimality, for some component $j$ it holds that

$$\lambda_A^j - pc_j = 0. \tag{12}$$

Assume first that $\lambda_A^j = \lambda_A^{\min}$. Then

$$p = \frac{\lambda_A^{\min}}{c_j}, \tag{13}$$

and because $\lambda_B^{\min} < c_{\min}$ it holds that

$$p = \frac{\lambda_A^{\min}}{c_j} < \frac{\lambda_A^{\min}}{\lambda_B^{\min}} = p_{\mathrm{up}}, \tag{14}$$

so the upper bound is not saturated.

Assume now that $\lambda_A^j \neq \lambda_{\min}^A = \lambda_A^l$ for some position $l \neq j$. Since

$$\lambda_A - p\lambda_C \geqslant 0 \tag{15}$$

it holds that

$$p \leqslant \min_i \frac{\lambda_A^i}{c_i}, \tag{16}$$

so since

$$p = \frac{\lambda_A^j}{c_j} \tag{17}$$

it holds that

$$p = \frac{\lambda_A^j}{c_j} \leqslant \frac{\lambda_A^l}{c_l} = \frac{\lambda_A^{\min}}{c_l} \leqslant \frac{\lambda_A^{\min}}{c_{\min}} < \frac{\lambda_A^{\min}}{\lambda_B^{\min}} = p_{\text{up}}. \tag{18}$$

Therefore, the upper bound is not attained and the lemma holds. ■

With Lemma 1 in place, we now show through an example that in the case of general amplification, the leakless case may not be optimal, and the upper bound $p_{\text{up}}$ can sometimes no longer be obtained. Consider amplification of a symmetric set of four coherent states from amplitude $\alpha = 2$ to amplitude $\beta = 2.3$. The eigenvalues of the corresponding Gram matrices are then given by

$$\lambda_A = [0.976\,39\,2, 0.971\,94\,2, 1.024\,28, 1.027\,39]^T, \tag{19}$$

$$\lambda_B = [1.005\,53, 0.991\,52\,7, 0.994\,52, 1.008\,42]^T, \tag{20}$$

and the upper bound is given with $p_{\text{up}} = 0.980\,24\,8$. Note that the smallest eigenvalue of the Gram matrix of the target states is unique, so Lemma 1 can be applied, and the upper bound cannot be reached in the leaky setting.

What remains to be seen is what the success probability of a leakless transform is. The leak of a leakless transform are kets with only global phases possibly differing. Lemma 4 in Ref. [21] can still be applied in this case; hence, we may assume that this leak is symmetric. This implies that the argument of the global phase of the $k$th ket is "symmetric" as well and will be of the form $\theta_k = \pi kj/2$ for $j = 0, \ldots, 3$. By the properties of the discrete Fourier transform of powers of roots of unity, the vector of eigenvalues of such a leak will be a vector with all components zero, except at the position $(4 - j \mod 4) + 1$, where its entry is 4.

A convolution of a vector comprising zeros, except at one position where the entry is one (or a constant $c$), with any other vector induces a circular permutation of the other vector (multiplied by the constant $c$). Hence, we can directly check the optimal leakless success probability of the leakless amplification procedure, by going through all the circular permutations of $\lambda_B$. We find that the optimal leakless transform succeeds with probability $p_{\text{leakless}} = 0.977\,29\,8 < p_{\text{up}}$. So, the upper bound cannot be reached for the leakless scenario either, which means that, surprisingly, it cannot be reached at all. We note that although the values used in this analysis are numerical, the discrepancies the conclusion relies on (i.e., the uniqueness of the smallest eigenvalue and comparison of magnitude of the quotients) are well within numerical precision; hence, the conclusion is unlikely to be a numerical artifact.

Now, is there a leaky transform that does not saturate the bound, but does better than the best leakless transform? Using the optimization technique developed in Ref. [21] we find that the success probability of an optimal transform for this example is $p_{\text{opt}} = 0.978\,60\,4$, which is slightly larger than the optimal leakless transform $p_{\text{leakless}} = 0.977\,29\,8$, and, necessarily, strictly below the upper bound $p = 0.980\,24\,8$.

To summarize, we have proven the following.

(1) The success probability of amplifying a symmetric set $A$ of $N$ coherent states of amplitude $\alpha$ to the states in a symmetric set $B$ of coherent states of a larger amplitude $\beta$, for small amplitudes $|\alpha| < |\beta| < 1$, can reach the upper bound imposed by the ratio of success probabilities of optimal unambiguous discrimination of sets $A$ and $B$, respectively.

(2) For small amplitudes $|\alpha| < |\beta| < 1$ the optimal transform is always leakless.

(3) The optimal success probability of amplification of small amplitudes is explicitly given by

$$p_{\text{opt}} = \frac{\sum_{r=0}^{\infty} \frac{\alpha^{2[N(r+1)-1]}}{[N(r+1)-1]!}}{\sum_{r=0}^{\infty} \frac{\beta^{2[N(r+1)-1]}}{[N(r+1)-1]!}}. \tag{21}$$

[Please see the Eq. (A6) in the Appendix, and the subsequent paragraph].

(4) If $|\beta| > 1$, the numerical testing we have performed indicates that the upper bound imposed by the ratio of the success probabilities for unambiguous discrimination of the states in sets $A$ and $B$ cannot always be reached, and optimal transforms may be leaky.

## V. CONCLUSIONS

In this work, we have shown that truly noiseless amplification of coherent states is possible if one only requires the amplification to work perfectly for a finite number of of states. Similarly, perfect cloning of any other linearly independent states is also possible, and amplification is clearly closely related to cloning. Depending on whether the amplitude of the amplified "target" states are below or above one, the optimal success probability may be simply obtained or require optimization techniques like the ones we developed in Ref. [21]. The average gain is, in principle, unlimited, since it is possible to base the amplification on USD. In case of success, this allows us to prepare an amplified state with arbitrary high amplitude. If we require a finite level of gain, the optimal success probability is higher than for unlimited gain. We have also explained how to implement truly noiseless amplification based on USD using only linear optics.

If we visualize the $N$ coherent states to be amplified as the ribs in an umbrella in an $N$-dimensional space, then noiseless amplification of these states, which decreases their pairwise overlaps, may be thought of as opening the umbrella. Sometimes the optimal amplification procedures may result in extra leak and redundancy states, apart from the desired amplified states. The leak and the redundancy may be correlated with and therefore carry information about the input state. Since the optimal umbrella transform for truly noiseless amplification is always leakless when the amplitude of the amplified (target) states is below one, as we have shown, this regime may be convenient if cryptographic aspects come into consideration.

For example, in a two-party protocol, where Alice sends some quantum states to Bob, who is supposed to further transform them, Alice can monitor the success probability declared by Bob. If it is optimal, she knows that there can be no additional leak (assuming that Alice uses some other way of checking that when Bob does declare that the process has succeeded, he has indeed obtained the quantum state he is supposed to). A related situation arises in blind quantum computing, where Alice wants to run a quantum computation on Bob's quantum computer without Bob learning about her data or her algorithm [10]. In the original scheme, Alice is required to prepare single-qubit states. If Alice only can prepare, say, weak coherent states, then one possibility may be for Alice to require Bob to turn these into single-qubit states in such a way that Alice can monitor any additional information Bob may gain. Such transforms from symmetric coherent states to symmetric qubit states were considered in Ref. [21]. If the amplitude of the target states is above one, then the optimal umbrella amplification transform may be leaky.

A few years ago, quantum cloning attracted widespread attention (see, e.g., Refs. [33–35]). Amplification and cloning are closely connected, especially for coherent states, since, for example, the state $|\alpha\rangle \otimes |\alpha\rangle$ may be transformed into $|\sqrt{2}\alpha\rangle$ using a beam splitter, and vice versa. More generally, if $g = \sqrt{N}$, then the state $|g\alpha\rangle$ is equivalent to $N$ copies of $|\alpha\rangle$, in the sense that $|\sqrt{N}\alpha\rangle$ can be transformed into $N$ copies of $|\alpha\rangle$ (and vice versa) by a linear optical network (a balanced multiport). It is well known that perfect universal quantum cloning, that is, of arbitrary states, is not possible [33,35], but cloning with imperfect fidelity is.

The fidelity of deterministic cloning can be improved if prior knowledge about the input states is available. Optimal cloning fidelity in the presence of prior knowledge for the case of cloning of CV systems, and in particular coherent states, has recently been addressed. Improvements have been shown, for instance, in settings where the input coherent states are picked from finite symmetric Gaussian distributions [17,18], have a fixed phase and a wide spread of possible mean photon numbers [17,18,20], or have a fixed mean photon number (but an arbitrary phase) [16,19]. In Ref. [16] it was shown that for the case of the latter type of prior knowledge—the so-called phase covariant cloning [19]—fidelity of the output clones can be further improved if the cloning process is allowed to be probabilistic and heralded. However, perfect fidelity is only reached in the limits of zero success probability, and/or zero amplitude.

On the other hand, probabilistic perfect cloning of linearly independent states is possible [36]. This mirrors the fact that probabilistic perfect amplification of linearly independent states is possible with finite success probability, as we have discussed.

To elaborate on the connection to cloning, the existing schemes for "noiseless" probabilistic amplification of coherent states are (almost) perfect cloners for coherent states, but do not clone superpositions of coherent states as well. For example, choosing $g = \sqrt{2}$, if $|\alpha\rangle \to |\sqrt{2}\alpha\rangle$ for any $\alpha$, then the "cat" state $N_\pm(|\alpha\rangle \pm |-\alpha\rangle)$ would change into $N'_\pm(|\sqrt{2}\alpha\rangle \pm |-\sqrt{2}\alpha\rangle)$, which may be transformed into $N'_\pm(|\alpha\rangle \otimes |\alpha\rangle \pm |-\alpha\rangle \otimes |-\alpha\rangle)$ using a balanced beam splitter. This state is not equal to $N_\pm(|\alpha\rangle \pm |-\alpha\rangle) \otimes N_\pm(|\alpha\rangle \pm |-\alpha\rangle)$, that is, to two copies of the original cat state. This is similar to the simple proof that universal cloning is impossible [33].

Nevertheless, this feature is not a disadvantage when perfect amplification schemes are used, for example, to enhance entanglement. That the operation $|\alpha\rangle \to |g\alpha\rangle$ only has unit fidelity in the limit of vanishing success probability, on the other hand, is a disadvantage. If we select a finite linearly independent set of states $|\alpha_i\rangle$ for which the amplification should work perfectly, then the fidelity of the probabilistic process $N \sum_i c_i|\alpha_i\rangle \to N' \sum_i c_i|g\alpha_i\rangle$ can be truly perfect, as we have pointed out. The price we have to pay is that the scheme *must* be dependent on phase and amplitude. Nevertheless, since such schemes can be realized with only linear optics, as discussed in Sec. II, we expect them to be of great interest for quantum information applications.

## ACKNOWLEDGMENTS

V.D. is fully and E.A. partially supported by EPSRC Grant No. EP/G009821/1.

## APPENDIX: PROPERTIES OF THE SPECTRUM OF THE GRAM MATRIX OF SYMMETRIC SETS OF COHERENT STATES

The vector of eigenvalues of the Gram matrix of a symmetric set of coherent states $\lambda_{G_A}$ can be obtained by the discrete Fourier transform of the first row of $G_A$ (for details, see Ref. [21]). Hence, the $j$th eigenvalue can be given as

$$\lambda_j = \sum_{l=0}^{N-1} \exp(-2jl\pi i/N)\, \langle\alpha|\alpha \exp(2l\pi i/N)\rangle. \quad \text{(A1)}$$

Using the expansion of the coherent states in the Fock number basis, the expression above can be written as

$$\lambda_j = \sum_{l=0}^{N-1} \exp\left(-\frac{2jl\pi i}{N}\right) \sum_{r=0}^{\infty} e^{-\alpha^2} \frac{\alpha^{2r}}{r!} \exp\left(\frac{2lr\pi i}{N}\right). \quad \text{(A2)}$$

This can further be rearranged as follows:

$$\begin{aligned} \lambda_j &= e^{-\alpha^2} \sum_{l=0}^{N-1} \sum_{r=0}^{\infty} \exp(-2jl\pi i/N) \frac{\alpha^{2r}}{r!} \exp(2lr\pi i/N) \\ &= e^{-\alpha^2} \sum_{r=0}^{\infty} \frac{\alpha^{2r}}{r!} \sum_{l=0}^{N-1} \exp(-2jl\pi i/N) \exp(2lr\pi i/n) \\ &= e^{-\alpha^2} \sum_{r=0}^{\infty} \frac{\alpha^{2r}}{r!} \sum_{l=0}^{N-1} \exp[2l(r-j)\pi i/N], \quad \text{(A3)} \end{aligned}$$

where to get to step (A3) we used the fact that the infinite sum is absolutely convergent, thereby allowing the commuting of sums.

By the properties of sums of roots of unity, the expression $\sum_{l=0}^{N-1} \exp[2l(r-j)\pi i/n]$ is equal to $n$ if $r-j$ is divisible by $N$ and zero otherwise. Hence, we obtain

$$\lambda_j = e^{-\alpha^2} N \sum_{r=0}^{\infty} \frac{\alpha^{2(Nr+j)}}{(Nr+j)!}. \quad \text{(A4)}$$

The elements in the sum above appear as the summands in the Taylor expansion of $e^{2\alpha}$. For any $j$ this sum collects every $N$th summand from the Taylor series expansion starting from the $j$th summand. We note that the eigenvalues above can be expressed in a closed form in terms of generalized hypergeometric functions. Using the presented form of the eigenvalues $\lambda_j$ we can show that for amplitudes below unity, the order of eigenvalues is monotonously decreasing.

*Lemma 2*. Let $A$ be the symmetric set of $N$ coherent states as defined in expression (3). Let $\lambda_A$ be the vector of eigenvalues of the Gram matrix $G_A$ generated by taking the discrete Fourier transform of the first row of $G_A$. If $\lambda_j$ is the $j$th component of $\lambda_A$, then for the real amplitude $\alpha \leqslant 1$ the eigenvalues in $\Lambda$ are decreasingly ordered:

$$\lambda_j \geqslant \lambda_{j+1}.$$

*Proof*. We will show that $\lambda_j - \lambda_{j+1} \geqslant 0$. By using expression (A4) derived above, we obtain

$$\begin{aligned}\lambda_j - \lambda_{j+1} &= e^{-\alpha^2} N \sum_{r=0}^{\infty} \frac{\alpha^{2(Nr+j)}}{(Nr+j)!} - e^{-\alpha^2} N \sum_{r=0}^{\infty} \frac{\alpha^{2(Nr+j+1)}}{(Nr+j+1)!} \\ &= e^{-\alpha^2} N \alpha^{2j} \sum_{r=0}^{\infty} \frac{\alpha^{2Nr}}{(Nr+j)!} \left(1 - \alpha^2 \frac{1}{Nr+j+1}\right),\end{aligned} \tag{A5}$$

where the last step is possible due to absolute convergence of the sums above. Note that the expression above is positive if $(1 - \alpha^2 \frac{1}{Nr+j+1})$ is positive. It holds that $Nr + j + 1 \geqslant 1$, so for $\alpha \leqslant 1$ the expression above is positive and we have our claim. Note also that in the case where $\alpha$ is strictly less than unity and positive, $\lambda_j$ is strictly greater than $\lambda_{j+i}$. So, for amplitudes below 1, the probability of success of unambiguous discrimination of symmetric sets of coherent states is given by the last eigenvalue in the vector $\lambda_A$. This eigenvalue is given by

$$\lambda_{\min} = e^{-\alpha^2} N \sum_{r=0}^{\infty} \frac{\alpha^{2(N(r+1)-1)}}{[N(r+1)-1]!}. \tag{A6}$$

In the case where Property 2 holds, from the equation above we can give the explicit optimal success probability of amplification of a set of symmetric coherent states. This is simply the quotient of the respective values of $\lambda_{\min}$ for the two amplitudes in the low-amplitude regime.

In the remainder of the Appendix we prove Property 2 from the main body of text. Let $\lambda_j(\alpha)$ be the $j$th eigenvalue of the Gram matrix of the symmetric set of $N$ coherent states of (real) amplitude $\alpha$. Property 2 states that

$$\frac{\lambda_j(\alpha)}{\lambda_j(\beta)} \geqslant \frac{\lambda_{N-1}(\alpha)}{\lambda_{N-1}(\beta)} \tag{A7}$$

for all $j = 0, \ldots, N-1$ and $0 < \alpha < \beta < 1$. Since all the eigenvalues are positive and nonzero, the inequality above can be rewritten as

$$\frac{\lambda_j(\alpha)}{\lambda_{N-1}(\alpha)} \geqslant \frac{\lambda_j(\beta)}{\lambda_{N-1}(\beta)}, \tag{A8}$$

which holds if and only if $\lambda_j(x)/\lambda_{N-1}(x)$ is a decreasing function on $(0,1)$. Note that the functions $\lambda_j(x)$ are non-negative for all $j$ on the interval of interest. If it is the case that $\lambda_j(x)/\lambda_{j+1}(x)$ is a decreasing function on the interval $(0,1)$ for all $j = 0, \ldots, N-2$, then the function $\lambda_j(x)/\lambda_{N-1}(x)$ is decreasing as well, which would imply Property 2. To see this, note that the equality

$$\frac{\lambda_j(x)}{\lambda_{j+1}(x)} \frac{\lambda_{j+1}(x)}{\lambda_{j+2}(x)} \cdots \frac{\lambda_{N-2}(x)}{\lambda_{N-1}(x)} = \frac{\lambda_j(x)}{\lambda_{N-1}(x)} \tag{A9}$$

holds for every $j$, and since the left-hand side of the expression above is a product of positive decreasing functions, the right-hand side must also be a decreasing function. Hence, it will suffice to show that $\lambda_j(x)/\lambda_{j+1}(x)$ is a decreasing function on the interval of interest, which we state as the following lemma.

*Lemma 3*. The quotient of eigenvalues

$$\frac{\lambda_j(x)}{\lambda_{j+1}(x)} \tag{A10}$$

is a decreasing function on $(0,1)$ for all $j = 0, \ldots, N-2$.

*Proof*. By recalling the analytic expression for the eigenvalues, given in Eq. (A4), we have

$$\begin{aligned}\frac{\lambda_j(x)}{\lambda_{j+1}(x)} &= \frac{e^{-x^2} N \sum_{r=0}^{\infty} \frac{x^{2(Nr+j)}}{(Nr+j)!}}{e^{-x^2} N \sum_{r=0}^{\infty} \frac{x^{2(Nr+j+1)}}{(Nr+j+1)!}} \\ &= \frac{\sum_{r=0}^{\infty} \frac{x^{2(Nr+j)}}{(Nr+j)!}}{\sum_{r=0}^{\infty} \frac{x^{2(Nr+j+1)}}{(Nr+j+1)!}}.\end{aligned} \tag{A11}$$

Let us introduce the notation

$$l_j(x) = \sum_{r=0}^{\infty} \frac{x^{2(Nr+j)}}{(Nr+j)!}.$$

To prove Lemma 3 we then need to show that $l_j(x)/l_{j+1}(x)$ is a decreasing function on $(0,1)$ for all $j = 0, \ldots, N-2$. Note that the functions $l_j(x)$ are positive, strictly increasing, and infinitely differentiable functions. Also, using the same technique we applied to prove the analogous property for the eigenvalues themselves, it holds that $l_j(x) \geqslant l_{j+1}(x)$ for all $j = 0, \ldots, N-2$, and for $x \in (0,1)$. Then, the quotient $l_j(x)/l_{j+1}(x)$ is decreasing in $x$ if and only if the derivative of the quotient over $x$ is nonpositive on the interval of interest:

$$\frac{l_j'(x) l_{j+1}(x) - l_j(x) l_{j+1}'(x)}{[l_{j+1}(x)]^2} \leqslant 0.$$

Since the denominator of the fraction above is always positive, this inequality holds if and only if the inequality

$$l_j'(x) l_{j+1}(x) - l_j(x) l_{j+1}'(x) \leqslant 0$$

holds.

It is easy to verify the following property of the derivatives of the functions $l_j(x)$:

$$l_j'(x) = \frac{d}{dx} l_j(x) = 2x l_{j-1 \bmod N}(x). \tag{A12}$$

Hence, we have

$$\begin{aligned}&l_j'(x) l_{j+1}(x) - l_j(x) l_{j+1}'(x) \\ &\quad = 2x [l_{j-1 \bmod N}(x) l_{j+1}(x) - l_j(x) l_j(x)],\end{aligned} \tag{A13}$$

which is nonpositive on the interval of interest if and only if

$$l_{j-1 \bmod N}(x) l_{j+1}(x) - l_j(x) l_j(x) \leqslant 0. \tag{A14}$$

Note that if $j = 0$ the expression above resolves to

$$l_{N-1}(x)l_1(x) - l_0(x)l_0(x) \leqslant 0. \tag{A15}$$

Since $l_{N-1}(x) \leqslant l_0(x)$ and $l_1(x) \leqslant l_0(x)$ on the interval $(0,1)$, and since all the values these functions attain are positive, we have that for $j = 0$ the condition given in expression (A14) holds. By using the definitions of the functions $l_j(x)$, for $j = 1,\ldots,N-2$, we obtain

$$\begin{aligned} & l_{j-1}(x)l_{j+1}(x) - l_j(x)l_j(x) \\ &= \sum_{r=0}^{\infty} \frac{x^{2(Nr+j-1)}}{(Nr+j-1)!} \sum_{r=0}^{\infty} \frac{x^{2(Nr+j+1)}}{(Nr+j+1)!} \\ &\quad - \sum_{r=0}^{\infty} \frac{x^{2(Nr+j)}}{(Nr+j)!} \sum_{r=0}^{\infty} \frac{x^{2(Nr+j)}}{(Nr+j)!} \end{aligned} \tag{A16}$$

$$\begin{aligned} &= x^{4j} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j-1)!} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j+1)!} \\ &\quad - x^{4j} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j)!} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j)!}. \end{aligned} \tag{A17}$$

The sign of the expression above is then equal to the sign of the expression

$$\begin{aligned} & \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j-1)!} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j+1)!} \\ &\quad - \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j)!} \sum_{r=0}^{\infty} (x^{2N})^r \frac{1}{(Nr+j)!}. \end{aligned} \tag{A18}$$

Note that to prove that $l_{j-1}(x)l_{j+1}(x) - l_j(x)l_j(x) \leqslant 0$ for $j > 0$ (and consequently Property 2), it suffices that the expression (A18) is negative for all $x \in (0,1)$, and for $j = 1,\ldots N-2$. Also, since any positive power is a bijection on the interval $x \in (0,1)$, and we require negativity on the entire interval, expression (A18) is negative if and only if the expression

$$\begin{aligned} & \sum_{r=0}^{\infty} (x^{N})^r \frac{1}{(Nr+j-1)!} \sum_{r=0}^{\infty} (x^{N})^r \frac{1}{(Nr+j+1)!} \\ &\quad - \sum_{r=0}^{\infty} (x^{N})^r \frac{1}{(Nr+j)!} \sum_{r=0}^{\infty} (x^{N})^r \frac{1}{(Nr+j)!} \end{aligned} \tag{A19}$$

is negative on the same interval.

Consider now the family of functions

$$f_j(x) = \sum_{r=0}^{\infty} \frac{x^{(Nr+j)}}{(Nr+j)!}.$$

Using the same construction as for the functions $l_j(x)$, it is easy to see that $f_j(x)/f_{j+1}(x)$ is a decreasing function on $(0,1)$ for $j = 1,\ldots,N-2$ if and only if the expression (A19) is negative on the same interval. For these functions $f_j$ it is also easy to see that they are positive, strictly increasing, and infinitely differentiable and that $f_j(x) \geqslant f_{j+1}(x)$ holds on the interval of interest for $j = 0,\ldots,N-2$. It also holds that

$$\frac{d}{dx} f_j(x) = f_{j-1 \bmod N}(x). \tag{A20}$$

Recall the property of log-concavity: A function is log-concave (on an interval) if the logarithm of that function is concave on the same interval. For functions which are twice differentiable, log-concavity holds if and only if the quotient of the derivative of the function and the function itself is decreasing (on the same interval). Hence, the requirement that $f_j(x)/f_{j+1}(x)$ is decreasing on the interval of interest is equivalent to the requirement that $f_{j+1}(x)$ is a log-concave function.

Here we invoke the following result given in Lemma 1 of the manuscript [37], also a consequence of the Lemma 3 in the Appendix of Ref. [38] (a published version of the aforementioned manuscript).

*Lemma 4*. Let $g(x)$ be a strictly monotonic, twice differentiable function on the interval $(a,b)$. Let also $g(a) = 0$ or $g(b) = 0$. Then if the derivative $g'(x)$ is log-concave on the same interval, $g(x)$ is log-concave on the interval.

Since for all $j > 0$ the function $f_j(0)$ is zero, and all the functions $f_j$ are strictly increasing, it holds that $f_{j+1}(x)$ is log-concave if $f_j(x)$ is log-concave. Inductively, if $f_1(x)$ is log-concave, so is $f_j(x)$ for all $j = 2,\ldots,N-1$. To finish the proof of Lemma 3 and thus of Property 2, we finally need to show that $f_1(x)$ is log-concave on $(0,1)$. Recall that $f_1(x)$ is log-concave on the interval of interest if the quotient $f_0(x)/f_1(x)$ is decreasing on the interval. This holds if the inequality

$$f_0'(x)f_1(x) - f_1'(x)f_0(x) = f_{N-1}(x)f_1(x) - f_0(x)f_0(x) \leqslant 0$$

holds. However, since we have that $f_j(x) \geqslant f_{j+1}(x)$ holds on the interval of interest for $j = 0,\ldots N-2$ and since all the functions above attain positive values, this inequality is satisfied. Hence, Lemma 3 and Property 2 are proven.

We note that the functions $l_j(x)$ and $f_j(x)$ are subseries of the Taylor expansion of the functions $e^{x^2}$ and $e^x$ about the point $x = 0$, respectively, and as such are absolutely convergent, which allows the unrestricted reshuffling of sums.


[1] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[2] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Photon. **4**, 316 (2010).

[3] M. A. Usuga, C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nat. Phys. **6**, 767 (2010).

[4] A. Zavatta, J. Fiurasek, and M. Bellini, Nat. Photon. **5**, 52 (2011).

[5] D. Menzies and S. Croke, arXiv:0903.4181.

[6] J. Jeffers, Phys. Rev. A **83**, 053818 (2011).

[7] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.

[8] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003).
[9] D. Sych and G. Leuchs, New J. Phys. **12**, 053019 (2010).
[10] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.
[11] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[12] P. J. Clarke, R. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller [Nat. Commun. (to be published)].
[13] A. Chefles, Phys. Lett. A **239**, 339 (1998).
[14] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[15] S. J. van Enk, Phys. Rev. A **66**, 042313 (2002).
[16] C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Phys. Rev. A **86**, 010305(R) (2012).
[17] P. T. Cochrane, T. C. Ralph, and A. Dolińska, Phys. Rev. A **69**, 042313 (2004).
[18] M. Sabuncu, G. Leuchs, and U. L. Andersen, Phys. Rev. A **78**, 052312 (2008).
[19] M. F. Sacchi, Phys. Rev. A **75**, 042328 (2007).
[20] Y. Dong, X. Zou, S. Li, and G. Guo, Phys. Rev. A **76**, 014303 (2007).
[21] V. Dunjko and E. Andersson, J. Phys. A: Math. Theor. **45**, 365304 (2012).
[22] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[23] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[24] A. Peres, Phys. Lett. A **128**, 19 (1988).
[25] S. M. Barnett and S. Croke, Adv. Opt. Phot. **1**, 238 (2009).
[26] J. A. Bergou, J. Mod. Opt. **57**, 160 (2010).
[27] A. Chefles, R. Jozsa, and A. Winter, arXiv:quant-ph/0307227.
[28] A. Chefles and S. M. Barnett, J. Phys. A **31**, 10097 (1998).
[29] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[30] A. Chefles, Phys. Rev. A **65**, 052314 (2002).
[31] A matrix is a Gram matrix of states if and only if it has unity across the diagonal and is positive semidefinite; see Ref. [27].
[32] A circulant matrix is a square matrix, whose $i$th row is the right cyclic shift of the $(i-1)$st row.
[33] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[34] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[35] A. Peres, arXiv:quant-ph/0205076.
[36] L. M. Duan and G. C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[37] M. Bagnoli and T. Bergstrom (1989), http://www.econ.ucsb.edu/~tedb/Theory/delta.pdf.
[38] M. Bagnoli and T. Bergstrom, Econ. Theory **26**, 446 (2005).
[39] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).